

## SECURITY MANAGEMENT METHOD FOR NETWORK SYSTEM

Patent Number: JP10269184  
Publication date: 1998-10-09  
Inventor(s): SAITO YOKO  
Applicant(s): HITACHI LTD  
Requested Patent: ☐ JP10269184  
Application Number: JP19970076954 19970328  
Priority Number(s):  
IPC Classification: G06F15/00 ; G06F1/00  
EC Classification:  
Equivalents:

### Abstract

**PROBLEM TO BE SOLVED:** To provide a security management method for facilitating transition from a present user authentication system by a user ID and a password to a single sign-on by the utilization of a certificate.

**SOLUTION:** A job is requested by transmitting the information of the certificate from a client 8 to a job server 6 and the confirmation of the certificate is requested by transmitting the information of the certificate from the job server 6 to an integrated authentication server 2. The integrated authentication server 2 confirms the certificate, then obtains the security information of a user from a server 3 and checks the right to access the job server 6 of the user. At the time of appropriate access, the user ID, the password and access-to- data control information are sent to the job server 6. The job server 6 performs the authentication processing on the user and manages the access right to data thereafter. It is similar for a DB(data base) server 5 as well.

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-269184

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl.<sup>\*</sup>G 0 6 F 15/00  
1/00

識別記号

3 3 0  
3 7 0

F I

G 0 6 F 15/00  
1/003 3 0 G  
3 7 0 E

審査請求 未請求 請求項の数 5 O L (全 13 頁)

(21) 出願番号 特願平9-76954  
(22) 出願日 平成9年(1997)3月28日

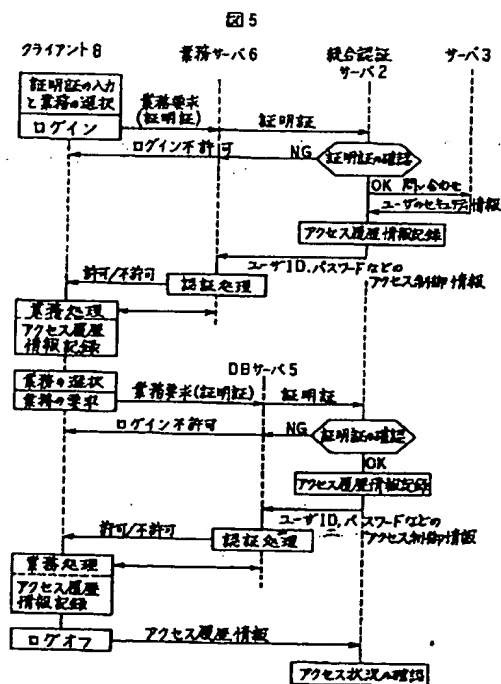
(71) 出願人 000005108  
株式会社日立製作所  
東京都千代田区神田駿河台四丁目6番地  
(72) 発明者 齋藤 洋子  
神奈川県横浜市戸塚区戸塚町5030番地 株  
式会社日立製作所ソフトウェア開発本部内  
(74) 代理人 弁理士 高橋 明夫

(54) 【発明の名称】 ネットワークシステムのセキュリティ管理方法

(57) 【要約】

【課題】 現行のユーザIDとパスワードによるユーザ認証方式から証明証の利用によるシングルサインオンへの移行を容易にするようなセキュリティ管理方法を提供する。

【解決手段】 クライアント8から業務サーバ6へ証明証の情報を送信して業務要求を行い、業務サーバ6から統合認証サーバ2へ証明証の情報を送信して証明証の確認要求を行う。統合認証サーバ2は、証明証の確認を行った後、サーバ3から当該ユーザのセキュリティ情報を取得してユーザの業務サーバ6へのアクセスする権限をチェックする。正当なアクセスであれば、業務サーバ6へユーザID、パスワード、データへのアクセス制御情報を送る。業務サーバ6はユーザの認証処理を行い、以後データへのアクセス権限を管理する。DBサーバ5についても同様である。



## 【特許請求の範囲】

【請求項1】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムのセキュリティ管理方法であって、クライアントから業務サーバへ証明証の情報を送信して業務要求を行い、業務サーバから統合認証サーバへ証明証の情報を送信して証明証の確認要求を行い、統合認証サーバによって証明証の確認とユーザの該業務サーバへのアクセス権限のチェックとを行い、正当であれば業務サーバへユーザIDとパスワードを送信し、該業務サーバによってユーザIDとパスワードによる認証を行うことを特徴とするセキュリティ管理方法。

【請求項2】統合認証サーバによって証明証の確認を行う代わりに、業務サーバによって証明証の確認を行い、業務サーバから統合認証サーバへ証明証の情報を送信してユーザIDとパスワードの要求を行い、統合認証サーバによってユーザの該業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへユーザIDとパスワードを送信し、該業務サーバによってユーザIDとパスワードによる認証を行うことを特徴とする請求項1記載のセキュリティ管理方法。

【請求項3】該クライアントによってシステムへのログインからログオフまでの間で該統合認証サーバ及び該業務サーバが実行する証明証の確認結果、該業務サーバへのアクセス権限のチェック結果、ユーザIDとパスワードの認証結果及び業務サーバが保持するデータへのアクセス権限のチェック結果を含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、該統合認証サーバによって証明証の確認結果及び該業務サーバへのアクセス権限のチェックを含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、該クライアントが記録するアクセス履歴情報と該統合認証サーバが記録するアクセス履歴情報とを突き合わせることによってユーザのアクセス状況をチェックすることを特徴とする請求項1記載のセキュリティ管理方法。

【請求項4】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムにおいて該統合認証サーバによって読み取り可能な記憶媒体上に実体化されたコンピュータプログラムであって、該プログラムは以下のステップを含む：(a) クライアントから業務サーバを経由して送信された証明証の情報を受信し、(b) 該証明証が正当であることを確認し、(c) 該証明証のユーザが該業務サーバにアクセスする権限があるか否かをチェックし、(d) (b) 及び (c) のチェック結果が妥当であれば該業務サーバによって該ユーザの認証を行うように該ユーザのユーザIDとパスワードを該業務サーバへ送信する。

【請求項5】ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムにおいて該統合認証サーバによって読み取

り可能な記憶媒体上に実体化されたコンピュータプログラムであって、該プログラムは以下のステップを含む：

- (a) クライアントから第1の業務サーバを経由して送信されたユーザIDとパスワードを受信し、(b) 該ユーザIDのユーザが第1の業務サーバにアクセスする権限があるか否かをチェックし、(c) (b) のチェック結果が妥当であれば該ユーザの一時的な証明証を作成し、(d) 第1の業務サーバを経由してクライアントへ該証明証を送信し、(e) クライアントから第2の業務サーバを経由して送信された該証明証の情報を受信し、(f) 該証明証が正当であることを確認し、(g) 該証明証のユーザが第2の業務サーバにアクセスする権限があるか否かをチェックし、(h) (f) 及び (g) のチェック結果が妥当であれば第2の業務サーバによって該ユーザの認証を行うように該ユーザのユーザIDとパスワードを第2の業務サーバへ送信する。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、クライアントとサーバを有するネットワークシステムのセキュリティ管理方法に係わり、特にユーザの一元管理を行い、ユーザに対して証明証を利用するシングルサインオン機能を提供するネットワークシステムのセキュリティ管理方法に関する。

## 【0002】

【従来の技術】インターネットの普及に伴ってセキュリティ管理をめぐる市場動向はめざましく変化している。特にインターネットのような広域ネットワークシステムと企業内ネットワークシステムとを結合するとき、これら両ネットワークを統合するようなユーザ認証機能及びネットワークシステム内の資源へのアクセスを制御する機能が求められている。すなわち広域ネットワークシステムと企業内ネットワークシステムの両者に亘ったユーザの一元管理とネットワーク資源の集中管理が望まれる。

【0003】広域ネットワークシステムを利用するユーザを一元管理する方法として、例えば特開平6-223041号公報に記載されるように利用者の個人情報と利用環境情報を秘密鍵によって暗号化した情報を証明書として発行し、利用者がこの証明書を利用してシステムにログインする方法がある。また分散システムを考慮するセキュリティ管理方法として、例えば特開平8-106437号公報に記載されるように、ユーザがそのホームドメインでないドメインへアクセスするときその資格認定を証明するログオン証明書を利用する方法がある。また特開平7-141296号公報は、ネットワークドメインをまたがってセキュリティを管理するTTP(Trusted Third Party)を設け、ネットワーク全体のセキュリティポリシーの設定、変更及びセキュリティポリシーに基づくアクセス制御を行うシス

ムを開示する。

【0004】

【発明が解決しようとする課題】以上述べたように証明証を利用してユーザ認証及びアクセス制御を行う方式は、今後の広域ネットワークシステムのセキュリティ管理方式の1つとして普及するものとみられる。しかし現実のネットワークシステムを考慮すると、現在の企業ネットワークシステムは、外部の証明証発行機関が発行する証明証を利用する方式にすぐに移行したり、TTPによるセキュリティ管理に移行するのが困難であると考えられる。すなわち現行のユーザIDとパスワードによるユーザ認証方式を残しながら証明証の利用によるシングルサインオン方式を導入していく方法が現実的と考えられる。

【0005】本発明の目的は、現行のユーザIDとパスワードによるユーザ認証方式から証明証の利用によるシングルサインオンへの移行を容易にするようなセキュリティ管理方法を提供することにある。

【0006】

【課題を解決するための手段】本発明は、ネットワークを介してクライアント、業務サーバ及び統合認証サーバが相互に通信可能なネットワークシステムのセキュリティ管理方法であって、クライアントから業務サーバへ証明証の情報を送信して業務要求を行い、業務サーバから統合認証サーバへ証明証の情報を送信して証明証の確認要求を行い、統合認証サーバによって証明証の確認とユーザの業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへユーザIDとパスワードを送信し、業務サーバによってユーザIDとパスワードによる認証を行うセキュリティ管理方法の特徴とする。

【0007】なお統合認証サーバによって証明証の確認を行う代わりに、業務サーバによって証明証の確認を行い、業務サーバから統合認証サーバへ証明証の情報を送信してユーザIDとパスワードの要求を行い、統合認証サーバによってユーザの業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへユーザIDとパスワードを送信し、業務サーバによってユーザIDとパスワードによる認証を行うようにしてもよい。

【0008】また本発明は、クライアントから業務サーバへユーザIDとパスワードを送信して業務要求を行い、業務サーバから統合認証サーバへ当該ユーザIDとパスワードを送信し、統合認証サーバによってユーザの業務サーバへのアクセス権限のチェックを行い、正当であれば一時的な証明証を作成して業務サーバを経由してクライアントへ送信するセキュリティ管理方法の特徴とする。

【0009】また本発明は、クライアントによってシステムへのログインからログオフまでの間で統合認証サーバ及び業務サーバが実行する証明証の確認結果、業務サーバへのアクセス権限のチェック結果、ユーザIDとバ

スワードの認証結果及び業務サーバが保持するデータへのアクセス権限のチェック結果を含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、統合認証サーバによって証明証の確認結果及び業務サーバへのアクセス権限のチェックを含むセキュリティ・チェックの結果をアクセス履歴情報として記録し、クライアントが記録するアクセス履歴情報と統合認証サーバが記録するアクセス履歴情報とを突き合わせることによってユーザのアクセス状況をチェックするセキュリティ管理方法の特徴とする。

【0010】さらに統合認証サーバによって読み取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して上記方法の統合認証サーバ側の処理を行うことができる。

【0011】

【発明の実施の形態】以下本発明の一実施形態について図面を用いて説明する。

【0012】図1は、本実施形態のネットワークシステムの構成図である。インターネットのような広域ネットワーク10には、企業ネットワークシステム1と他企業ネットワークシステム9が接続される。企業ネットワークシステム1には、クライアント8のほかに、統合認証サーバ2、セキュリティ情報を管理するサーバ3、データベース(DB)サーバ5、業務サーバ6、グループウェアサーバ4、鍵管理サーバ17、証明証発行サーバ18等のサーバが接続される。DBサーバ5及び業務サーバ6は、クライアント8からアクセスされ、業務処理のために利用されるサーバである。グループウェアサーバ4は、クライアント8へ最初の業務メニュー画面を送ったり、クライアント8へ電子メールを送ったり、ユーザのスケジュールを管理するサーバである。サーバ3はDBサーバ5及び業務サーバ6へのアクセスを制御する情報とユーザIDとパスワードのような認証情報を含むユーザのアクセス制御情報とから成るセキュリティ情報を一元的に管理するサーバである。統合認証サーバ2は、クライアント8から送られる証明証を確認し、サーバ3からセキュリティ情報を取得してユーザのDBサーバ5及び業務サーバ6へのアクセス権限をチェックするサーバである。鍵管理サーバ17は、企業ネットワークシステム1内での暗号化通信で使用するマスタ鍵を生成するサーバである。広域ネットワーク10には外部証明証発行サーバ7が接続される。外部証明証発行サーバ7は、所定の手順に従って外部証明証を発行するサーバである。証明証発行サーバ18は、統合認証サーバ2からの要求によって外部証明証をもたないユーザに対して証明証を発行するサーバである。なおいわゆるディレクトリサーバと呼ばれるサーバがサーバ3の情報を有していてもよい。またクライアント8及び各種サーバは、パソコン、ワークステーション等を含む情報処理装置である。さらにクライアント8及び各種サーバによって各々読み

取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して以下に詳述するクライアント8及び各種サーバの処理を行うことができる。

【0013】クライアント8又は他企業ネットワークシステム9に接続されるクライアント20からユーザの証明証の情報を入力して例えばDBサーバ5にログインすると、DBサーバ5又は統合認証サーバ2が証明証の確認を行い、統合認証サーバ2がサーバ3からセキュリティ情報を取得してDBサーバ5へのアクセス権限をチェックする。アクセス権限があれば、DBサーバ5へユーザID、パスワードなどの認証情報を送り、DBサーバ5がユーザの認証処理を行う。DBサーバ5を利用する業務処理が終了し、次に業務サーバ6にログインするとき、クライアント8はすでに入力済みの証明証を業務サーバ6に送信し、上記の手続きを行うことによってシングルサインオンが実現する。証明証をもたないユーザに対しては、ユーザIDとパスワード入力によるログインによって証明証を発行し、以後クライアント8は、別の業務サーバに移ることにこの証明証を業務サーバへ送信し、シングルサインオンが可能である。

【0014】図2は、セキュリティ情報を管理するサーバ3がセキュリティ情報を一元管理する方式を説明する図である。サーバ3を導入する前に各サーバごとに管理していたユーザ及び資源（文書、データベース、端末装置、アプリケーションプログラム等）に関するセキュリティ情報をLDAP情報交換プログラムによってLDAP形式に変換し、サーバ3へ送ってサーバ3で一元管理する。ここにLDAP（Lightweight Data Access Protocol）は、IETF標準のディレクトリアクセスプロトコルである。

【0015】図3は、LDAP形式の情報の例として、文書の定義と業務サーバのアクセス制御情報の形式を示す図である。文書の定義は、文書識別情報と文書のアクセス制御情報から構成される。文書識別情報は、文書の識別子、この文書を管理するサーバの識別子と組織名称並びに文書の情報（文書のタイトル、文書の更新日付、文書管理者、文書検索のためのキーワード、主題、アブストラクト、作者名）から構成される。一方文書のアクセス制御情報は、アクセス制御情報、最終修正情報、セキュリティポリシー等を含む。アクセス制御情報は文書内の特定ページのアクセス制御情報のように文書の一部についてアクセス制御をする情報である。最終修正情報はアクセス制御情報の更新日付である。セキュリティポリシーはその文書にアクセスを許可するユーザのアクセスレベルを設定するものである。例えばポリシー番号が1から3までのユーザに該当文書をアクセス許可するという運用が可能である。文書の定義は、業務サーバ6が管理する情報である。

【0016】業務サーバのACL（Access Control List：アクセス制御リスト）情報とし

て、業務サーバ6をアクセスするときのアクセス制御情報、アクセス制御情報の管理元サーバの識別子、ドメインセキュリティの定義の更新日付、セキュリティポリシーとしてデフォルトセキュリティポリシー及び認可セキュリティポリシー、及び経由するDSA（Domain Security Authority）を定義している。認可セキュリティポリシーは、例えばポリシー番号が1から5までのユーザに業務サーバ6のアクセスを許可するという運用が可能である。経由するDSAによれば、ユーザの認証は必ず統合認証サーバ2を経由して行うよう定義する。業務サーバのアクセス制御情報は、サーバ3が保持し、統合認証サーバ2が管理する情報である。

【0017】なお上記のアクセス制御情報のほかに、業務サーバ6にアクセスし、特定の文書にアクセスするユーザについてもアクセス制御情報を設定する必要がある。ユーザのアクセス制御情報は、ユーザの証明証の情報、ユーザIDとパスワードのような認証情報、ユーザの属する部門と職制情報、ユーザのアクセスレベル（ポリシー番号）等を設定する。アクセスレベルの設定によって、例えばポリシー番号が4のユーザは業務サーバ6にはアクセス可能であるが、XXXXという文書へのアクセスを許可しないという運用が可能である。またある職制以上のユーザに対して特定の文書のアクセスを許可するような運用も可能である。

【0018】図4は、統合認証サーバ2がサーバ3からユーザのセキュリティ情報を取得する手順を示す図である。セキュリティ情報を取得する手順には、LDAPプロトコルが使用される。統合認証サーバ2は、まずldap\_openによってサーバ3とLDAPコネクションを確立し、ldap\_simple\_bind\_sによって統合認証サーバ2とサーバ3との間の相互認証を行った後、ldap\_search\_sによって統合認証サーバ2からユーザの証明証番号、ユーザIDなどを送信すると、サーバ3から統合認証サーバ2へそのユーザのセキュリティ情報を送信する。

【0019】図5は、クライアント8のユーザが企業ネットワークシステム1にログインしてからログオフするまでの処理の手順を示す図である。ここではユーザが証明証（外部証明証を含む）を用いてログインする場合の手順について説明する。クライアント8は、業務メニューをクライアント8の表示装置に表示する。ユーザが業務サーバ6を選択し、証明証の情報をICカード等の記憶媒体から入力すると、クライアント8は、証明証の情報をユーザの秘密鍵で暗号化して記憶装置に格納した後、業務要求とユーザの秘密鍵で暗号化された証明証の内容を業務サーバ6へ送信する。業務サーバ6は、統合認証サーバ2へ証明証の情報を送りその内容の確認要求を行う。統合認証サーバ2は、暗号化された証明証をユーザの公開鍵で復号化した後、その証明証の確認を行

う。証明証のデータ構成はX. 509で規定されており、その内容は所有者氏名、発行元、発行元の署名、有効期限等の情報から成る。発行元の署名は発行者の秘密鍵で暗号化されているので、まずこの署名を発行元の公開鍵で復号して原本と比較し、証明証が正当なものであることを確認する。次に有効期限等内容の確認を行う。証明証が不適当なものであれば(NG)、業務サーバ6を経由してクライアント8へログイン不許可のメッセージを送信する。証明証が適当なものであれば(OK)、サーバ3へ問い合わせを行ってユーザのセキュリティ情報を取得する。その手順については上記した通りである。ユーザのセキュリティ情報は、業務サーバ6のアクセス制御情報とユーザのアクセス制御情報から構成される。統合認証サーバ2は、ユーザのアクセスレベルと業務サーバ6のアクセスレベルとを比較し、業務サーバ6のアクセスを許可できるならば、当該ユーザのアクセスを許可する旨のアクセス履歴情報を記憶装置に記録し、業務サーバ6へ暗号化したユーザID、パスワード、アクセスレベル、職制情報などユーザのアクセス制御情報を送信する。なお業務サーバ6がユーザIDに対応してアクセスレベル、職制情報などユーザのアクセス制御情報を保有している場合には、ユーザIDとパスワード以外のアクセス制御情報の送信は不要である。業務サーバ6は、受信したアクセス制御情報を復号し、まずユーザIDとパスワードが登録されているものに一致するか否か認証処理を行う。一致しなければ業務サーバ6へのアクセスを許可しない。一致すればクライアント8へ許可のメッセージを送信する。以後クライアント8から文書のアクセス要求があるごとに文書のアクセス制御情報とユーザのアクセスレベル、職制情報とから文書のアクセスを許可するか否かを決定する。クライアント8からは業務サーバ6が保有する文書にアクセス要求をして業務処理を行う。クライアント8は、業務処理の間、アクセスする文書についてアクセス履歴情報を記憶装置に記録する。

【0020】このようにして業務サーバ6に係わる業務処理を終了した後、再び業務メニューをクライアント8の表示装置に表示する。ユーザが次にDBサーバ5を選択したとすれば、クライアント8は記憶していた当該ユーザの証明証を取り出して業務要求とともにDBサーバ5へ送信する。従ってユーザは再度証明証の情報を入力する必要がない。DBサーバ5は、統合認証サーバ2へ証明証の情報を送りその内容の確認要求を行う。以後上記と同様に統合認証サーバ2は、暗号化された証明証をユーザの公開鍵で復号化した後、証明証の確認を行い、証明証の確認結果と当該ユーザのDBサーバ5へのアクセスを許可/不許可する旨のアクセス履歴情報を記録し、DBサーバ5へアクセス制御情報を送信する。DBサーバ5は、ユーザIDとパスワードによってユーザの認証処理を行う。ユーザのアクセスを許可したとき、以

後受信したアクセス制御情報に基づいて指定されたデータベース、テーブル、テーブルの列などのアクセスを許可するか否かを決定する。クライアント8は、DBサーバ5を利用して業務処理を行い、業務処理の間、アクセスするデータベースについてアクセス履歴情報を記録する。このようにして業務処理が終了し、ユーザがログオフを入力すると、クライアント8は記録したアクセス履歴情報を統合認証サーバ2へ送り、記憶装置上に保管していた証明証の情報を消去する。統合認証サーバ2は、受信したアクセス履歴情報と統合認証サーバ2が記録したアクセス履歴情報を比較して妥当なアクセスであるか否かチェックする。

【0021】なお図5の処理手順において、最初に業務サーバ6にログインする代わりにグループウェアサーバ4にログインする場合も同様の処理手順になる。

【0022】図6は、業務サーバ6及びDBサーバ5が証明証の内容を確認する機能をもつ場合の処理の手順を示す図である。図6の手順が図5の手順と異なる点は、統合認証サーバ2の代わりに業務サーバ6及びDBサーバ5がユーザの秘密鍵で暗号化された証明証をユーザの公開鍵で復号化した後、証明証を確認する点である。各業務サーバが証明証の内容を確認するためには、証明証の発行元の公開鍵を取得し、発行元の署名を確認する機能が必要である。

【0023】図7は、証明証をもたないユーザが企業ネットワークシステム1にログインしてからログオフするまでの処理の手順を示す図である。ユーザが業務メニューの中から業務サーバ6を選択し、ユーザIDとパスワードを入力すると、クライアント8は、業務要求とユーザID、パスワードを業務サーバ6へ送信する。業務サーバ6は受け取ったユーザIDとパスワードが登録されているものに一致するか否か認証処理を行う。一致していなければ業務サーバ6へのアクセスを拒否する。一致しているとき業務サーバ6は、統合認証サーバ2へ受信したユーザIDとパスワードを送る。統合認証サーバ2は、サーバ3へユーザIDとパスワードを送って問い合わせを行い、ユーザのセキュリティ情報を取得する。次に統合認証サーバ2は、サーバ3から受け取ったセキュリティ情報に基づく上記のチェック処理によってユーザが業務サーバ6にアクセスする権限があるか否かチェックする。ユーザに権限がなければ(NG)、クライアント8へログイン不許可のメッセージを送信する。ユーザに権限があれば(OK)、証明証を発行する。この証明証は一時的に業務サーバ6へのアクセスを許可する目的で発行されるものなので、その有効期限は通常の証明証より短く(例えば当日限りなど)、業務サーバ6へのアクセス権限も制限される。次に統合認証サーバ2は、業務サーバ6へ証明証とアクセスレベル、職制情報などユーザのアクセス制御情報を送信する。業務サーバ6がアクセス制御情報を保有している場合には、アクセス制御

情報の送信は不要である。業務サーバ6は、受信した証明証をクライアント8へ送信する。クライアント8は、受信した証明証を記憶装置に格納したのち、業務サーバ6が保有する文書にアクセス要求をして業務処理を行う。業務サーバ6は、クライアント8から文書のアクセス要求があるごとに文書のアクセス制御情報とユーザのアクセスレベル、職制情報とから文書のアクセスを許可するか否かを決定する。クライアント8は、業務処理の間、アクセスする文書についてアクセス履歴情報を記録する。またクライアント8は、周期的に証明証の有効期限をチェックし、有効期限を過ぎる場合にはユーザに警告する。

【0024】このようにして業務サーバ6に係わる業務処理を終了した後、ユーザがDBサーバ5を選択した場合、クライアント8は保管していた証明証を取り出して業務要求とともにDBサーバ5へ送信する。DBサーバ5は、統合認証サーバ2へ証明証の情報を送り、その内容の確認要求を行う。統合認証サーバ2は、上記のように証明証の確認を行い、DBサーバ5へユーザID、パスワードを含むアクセス制御情報を送信する。DBサーバ5は、ユーザID、パスワードによる認証処理を行い、正当であればDBサーバ5へのアクセスを許可する。以後上記のようにクライアント8はDBサーバ5にデータベースのアクセス要求を送信し、DBサーバ5はユーザのアクセス制御情報に基づいてデータベースのアクセスを許可するか否かを決定する。クライアント8はDBサーバ5を利用して業務処理を行い、業務処理の間、アクセスするデータベースについてアクセス履歴情報を記録する。このようにして業務処理を終了し、ユーザがログオフを入力すると、クライアント8は記録したアクセス履歴情報を統合認証サーバ2へ送り、保管していた証明証の情報を消去する。統合認証サーバ2は、受信したアクセス履歴情報と統合認証サーバ2が記録したアクセス履歴情報とを比較して妥当なアクセスであるか否かチェックする。ログオフ手続きの一環としてユーザから証明証の発行要求があれば、クライアント8はこの要求を統合認証サーバ2へ送信する。統合認証サーバ2は、当該ユーザのセキュリティ情報とアクセス状況に問題があるか否かチェックする。すなわち統合認証サーバ2がユーザの権限確認の後のアクセス履歴情報にログイン許可の記録がなければ、当然問題ありとなる。またその後のDBサーバ5のアクセス許可の記録がないにもかかわらずクライアント8側のアクセス履歴情報にDBサーバ5にアクセスした記録がある場合にも問題ありとなる。またクライアント8が業務サーバ6及びDBサーバ5の文書やデータベースにアクセスするとき不許可のケースがクライアント8側のアクセス履歴情報に記録されていれば問題が生じている。問題があるとき(YES)、統合認証サーバ2は、クライアント8へ証明証の発行を許可しない旨のメッセージを送信する。問題がな

ければ(NO)、統合認証サーバ2は、証明証発行サーバ18へ証明証の発行要求を送信し、証明証発行サーバ18が証明証を発行して統合認証サーバ2へ送信し、統合認証サーバ2がこの証明証をクライアント8へ送信する。クライアント8は受信した証明証をICカード、フロッピーディスク等の外部記録媒体に出力する。この後ユーザは、図5に示す証明証を用いるログイン手続きを行うことができる。このように本実施形態によれば、証明証をもたないユーザがログインする場合も1回のログインによるシングルサインオンを実現できる。なお統合認証サーバ2、業務サーバ6及びDBサーバ5は、図5に示す処理手順と図7に示す処理手順の両方を併行してサポートするのが望ましい。

【0025】図8は、統合認証サーバ2がユーザのアクセス状況を監視してセキュリティ侵害を検出する処理の手順を示す図である。クライアント8と統合認証サーバ2が連携することによってユーザのアクセス状況をチェックし、システムへのセキュリティ侵害を検出することが可能である。図8の例ではクライアント8が業務サーバ6にアクセスして業務処理を行っているとき、ある文書についてアクセス要求をすると、業務サーバ6がユーザのアクセス制御情報と文書のアクセス制御情報とからアクセスチェックを行い、その結果不当なアクセス要求であればクライアント8へアクセス不許可のメッセージを返す状態を示している。クライアント8は、このアクセス不許可をアクセス履歴情報に記録する。クライアント8がログオフを指示すると、クライアント8で記録された当該ユーザについてのアクセス履歴情報を統合認証サーバ2へ送信する。統合認証サーバ2は、統合認証サーバ2が採取したアクセス履歴情報、クライアント8が採取したアクセス履歴情報及び両者の突き合わせからユーザのアクセス状況が正当か否かを判定する。もしユーザが不当なアクセス又は不適切なアクセスをしていると判定すれば、統合認証サーバ2は当該ユーザのアクセス制御情報を削除する処理を行う。

【0026】ユーザの不当なアクセス又は不適切なアクセスとして例えば次のようなケースがある。

(a) 統合認証サーバ2にログイン許可の記録がない。すなわち証明証の確認結果が不許可である。

(b) 統合認証サーバ2が行うユーザの権限確認チェックの結果、業務サーバへのアクセスを不許可にしているにもかかわらずクライアント8がその業務サーバにアクセスしている。

(c) 業務サーバ又はDBサーバが行う認証処理の結果が不許可である。

(d) クライアント8が証明証の有効期限の期限切れを検出している。

(e) クライアント8が許可されない文書やデータベースへのアクセスを試行している。

(f) クライアント8が証明証を入力した時刻、ログイ



ン指令をした時刻、統合認証サーバ2が証明証を確認した時刻、業務サーバ6がユーザの認証を行って業務サーバ6へのアクセスを許可した時刻などアクセス履歴情報に記録されたセキュリティ関係の処理時刻が正しい時系列のシーケンスになっていない。

【0027】本実施形態によれば、統合認証サーバ2及びサーバ3がユーザのアクセス制御情報と業務サーバのアクセス制御情報とから成るセキュリティ情報を一元管理するため、セキュリティ情報の登録と更新を集中的に行うことができ、従来のように各業務サーバがセキュリティ情報を個別に管理する必要がない。

【0028】図9は、セキュリティ情報の登録、照会及び更新の手順を示す図である。図9(a)は、セキュリティ情報の登録フェーズの処理手順を示す図である。各サーバからサーバ3へセキュリティ情報の登録を要求すると、サーバ3は要求されたセキュリティ情報を記憶装置に登録する。このとき上述したようにLDAP情報交換プログラムを利用して既存のセキュリティ情報をLDAP形式に変換することができる。図9(b)は、セキュリティ情報の照会の手順を示す図である。各サーバから統合認証サーバ2へセキュリティ情報を問い合わせる。統合認証サーバ2は、指定されたユーザに関するセキュリティ情報をすでに取り込んでいれば(YES)、そのセキュリティ情報を回答する。取り込んでなければ(NO)、サーバ3に問い合わせてセキュリティ情報を取得してから要求元のサーバに回答する。例えば図6に示す業務サーバ6及びDBサーバ5が証明証情報を統合認証サーバ2へ送信してセキュリティ情報を照会する場合がこれに相当する。また図7に示す業務サーバ6がユーザIDとパスワードを統合認証サーバ2へ送信してユーザの権限確認を依頼し、証明証の発行を依頼し、ユーザのアクセス制御情報を受ける場合もこれに相当する。図9(c)は、セキュリティ情報の更新の例を示す図である。統合認証サーバ2がユーザによるセキュリティ侵害を検出したとき、各サーバへユーザの削除を通知する。またサーバ3へ当該ユーザについてアクセス制御情報の削除を要求する。

【0029】なお統合認証サーバ2とサーバ3を分離せずに同一のサーバにしても本発明を実現できる。また統合認証サーバ2、サーバ3、鍵管理サーバ17及び証明証発行サーバ18を同一のサーバで実現することも可能である。

【0030】最後にクライアント8、サーバ5、6及び統合認証サーバ2との間の暗号化通信について説明する。従来のユーザ情報、特にパスワード情報が通信回線上で盗聴されると、盗んだ情報を基にして他人に成りすましたりするセキュリティ上の脅威があった。本発明は、本来公開されて良い証明証の情報をを用いてユーザを確認するため、証明証の情報に加えてユーザの秘密鍵の情報が盗まれれば悪意のある第三者が他人に成りすま

ことも有り得る。従ってクライアント8、サーバ5、6及び統合認証サーバ2との間の通信は、相互に通信相手の認証をした後に、暗号化通信により行われる必要がある。特に各サーバと統合認証サーバ2の間ではユーザに関するセキュリティ情報が送受信されるために、当事者だけが見られるように情報を保護する必要がある。セキュリティ情報を保護するための通信手段として、例えばSSL(Secure Socket Layer)が知られている。

【0031】暗号化通信を行うためには、暗号鍵の生成、配送及び回復のような鍵管理の問題がある。どのような暗号化手段を用いるかによって管理方法や実現方法が異なる。以下にMulti2と呼ばれるグループ鍵暗号方式による暗号化技術について説明する。

【0032】図10は、グループ鍵によるデータの暗号化処理の手順を説明する図である。鍵管理サーバ17は、クライアント、及びサーバのマスター鍵を作成し配布する。そしてこのマスター鍵からメッセージを暗号化するために暗号鍵を生成するが、当メッセージを読ませたい相手(複数の指定が可能)を宛て先リストに登録し、マスター鍵と宛て先リストから動的にグループ鍵を作成し、このグループ鍵によってメッセージを暗号化する。図10の例では、クライアント8は、業務サーバ6にメッセージAを送信する際に宛て先リストAにクライアント8、業務サーバ6及び統合認証サーバ2を指定する。そして業務サーバ6に対してはグループ鍵Aを送信せず、メッセージAを暗号化したものと宛て先リストAだけを送る。業務サーバ6は、クライアント8から受信したメッセージAを復号化するために、メッセージAとともに受信した宛て先リストAとマスター鍵から動的にグループ鍵Aを作成する。業務サーバ6は、このようにして作成したグループ鍵AによりメッセージAを復号化する。また業務サーバ6から統合認証サーバ2へメッセージAを送信する場合にも、マスター鍵と宛て先リストAからグループ鍵Aを作成し、送信したいメッセージAをグループ鍵Aで暗号化する。グループ鍵Aは、宛て先リストAに登録され、かつマスター鍵を持つ相手でなければ動的に作成できないため、このように見せたい相手だけにメッセージAを読ませることができる。

【0033】次に統合認証サーバ2が業務サーバ6へメッセージBを送信したい場合には、宛て先リストBに業務サーバ6だけを設定し、マスター鍵と宛て先リストBから作成したグループ鍵BによってメッセージBを暗号化して送る。クライアント8がこの暗号化されたメッセージBを解読しようとしても、クライアント8は宛て先リストBに登録されていないために解読することができない。図10の例では、クライアント8と各サーバ間のグループ鍵による暗号化通信を説明したが、ユーザごとにマスター鍵を持たせることも可能である。この場合には、マスター鍵をICカード内に格納し、ICカード中でグル



ープ鍵を生成することも可能である。

【0034】

【発明の効果】以上述べたように本発明によれば、業務サーバやデータベースサーバが従来のユーザIDとパスワードに基づくユーザ認証とアクセス制御を保存しながらユーザに対して証明証利用によるシングルサインオンの機能を提供できる。また証明証をもたないユーザに対しても一時的な証明証の発行によるシングルサインオンを実現することができる。またクライアントと統合認証サーバが連携することによって、ユーザのアクセス状況を監視し、アクセス状況に問題があるユーザをシステムから除外することができる。

【図面の簡単な説明】

【図1】実施形態のネットワークシステムの構成図である。

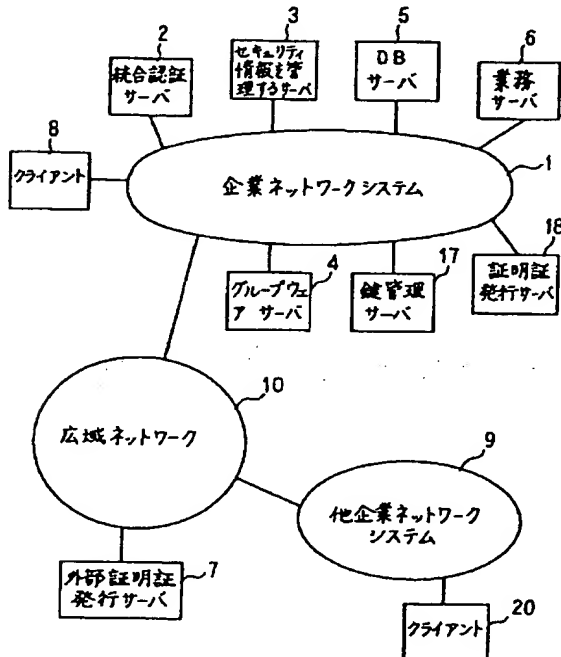
【図2】実施形態のサーバ3がセキュリティ情報を一元管理する方式を説明する図である。

【図3】LDAP形式の情報の例を示す図である。

【図4】実施形態の統合認証サーバ2がサーバ3からユ\*

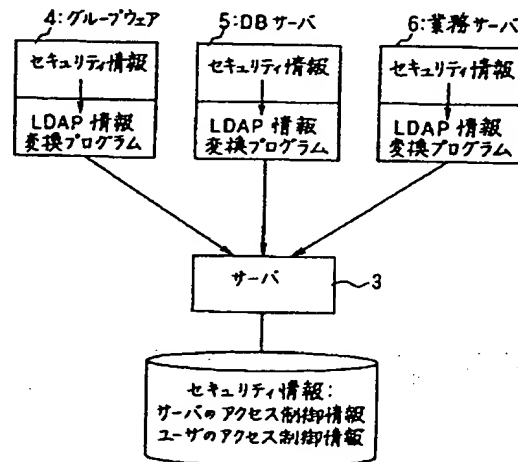
【図1】

図1



【図2】

図2



\* ユーザのセキュリティ情報を取得する手順を示す図である。

【図5】実施形態の証明証を利用するシングルサインオンの処理手順を示す図である。

【図6】図5の処理手順で統合認証サーバ2の代わりにDBサーバ5/業務サーバ6が証明証を確認する処理手順を示す図である。

【図7】実施形態の証明証をもたないユーザによるシングルサインオンの処理手順を示す図である。

10 【図8】実施形態の統合認証サーバ2がユーザのアクセス状況を監視してセキュリティ侵害を検出する処理手順を示す図である。

【図9】実施形態のセキュリティ情報を管理する処理を説明する図である。

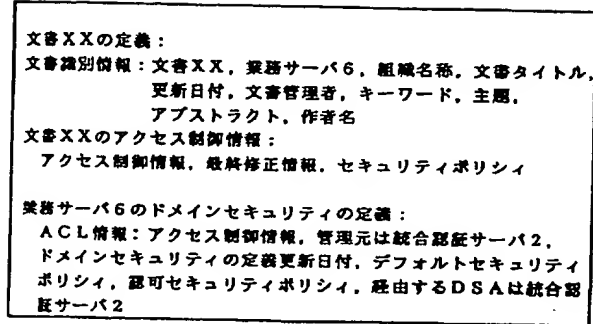
【図10】グループ鍵によるデータの暗号化処理の手順を説明する図である。

【符号の説明】

2：統合認証サーバ、3：（セキュリティ情報を管理する）サーバ、18：証明証発行サーバ

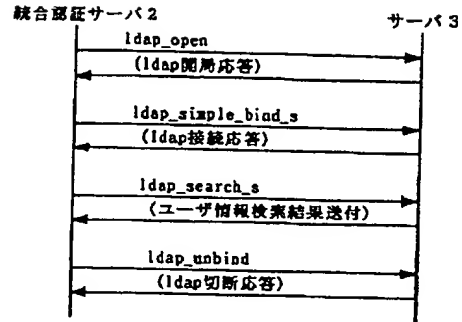
【図3】

図 3



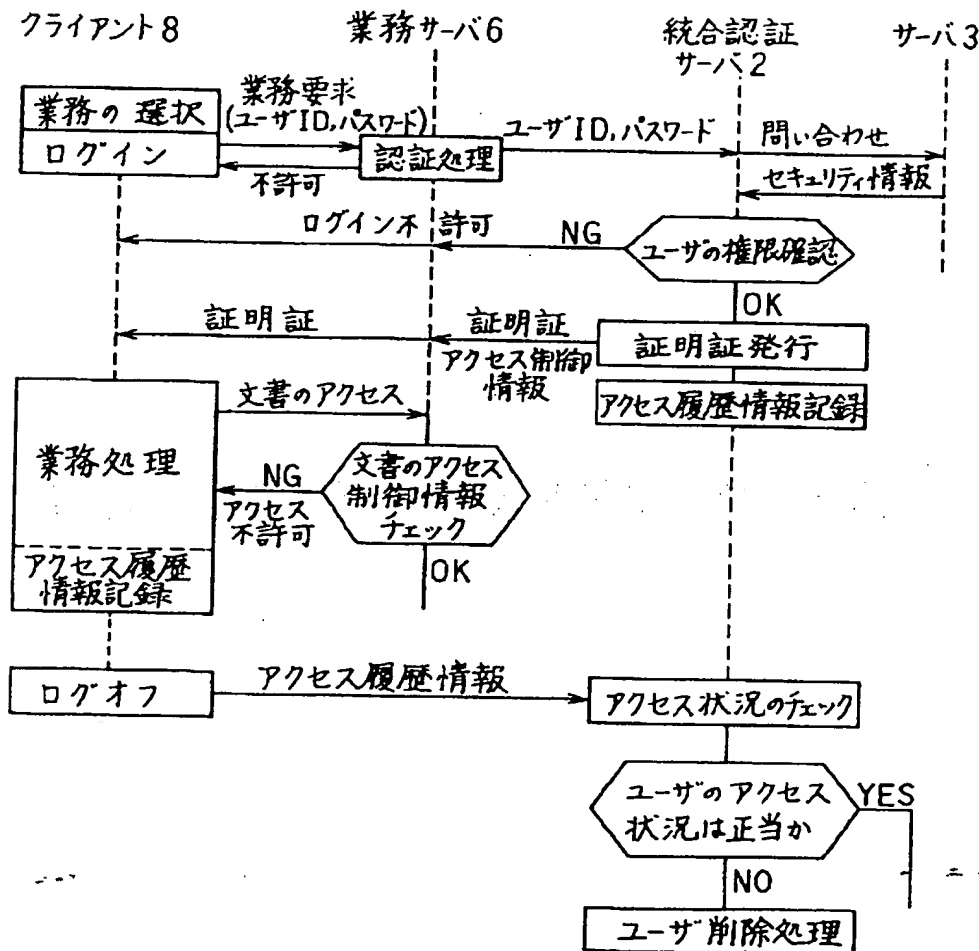
【図4】

図 4



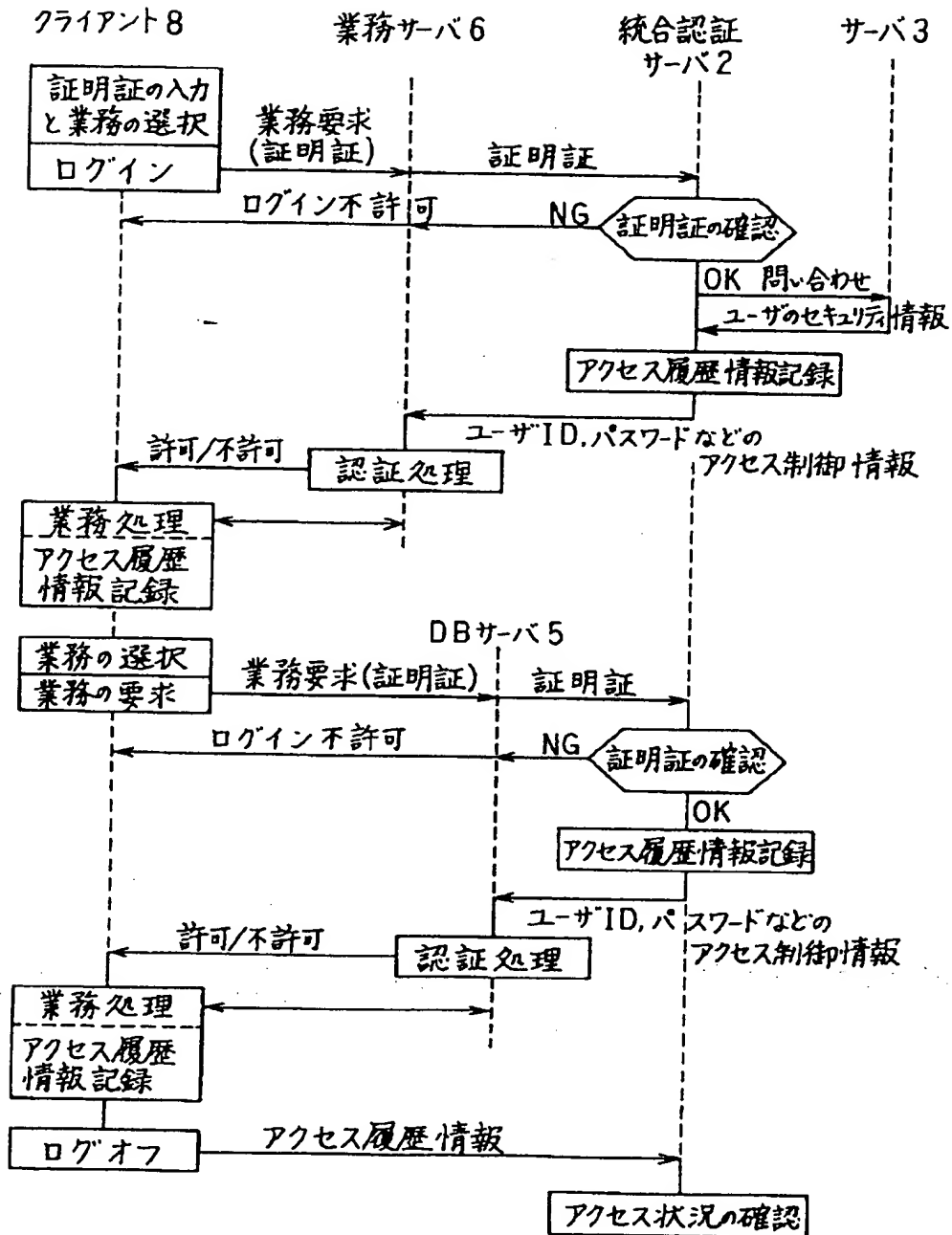
【図8】

図 8



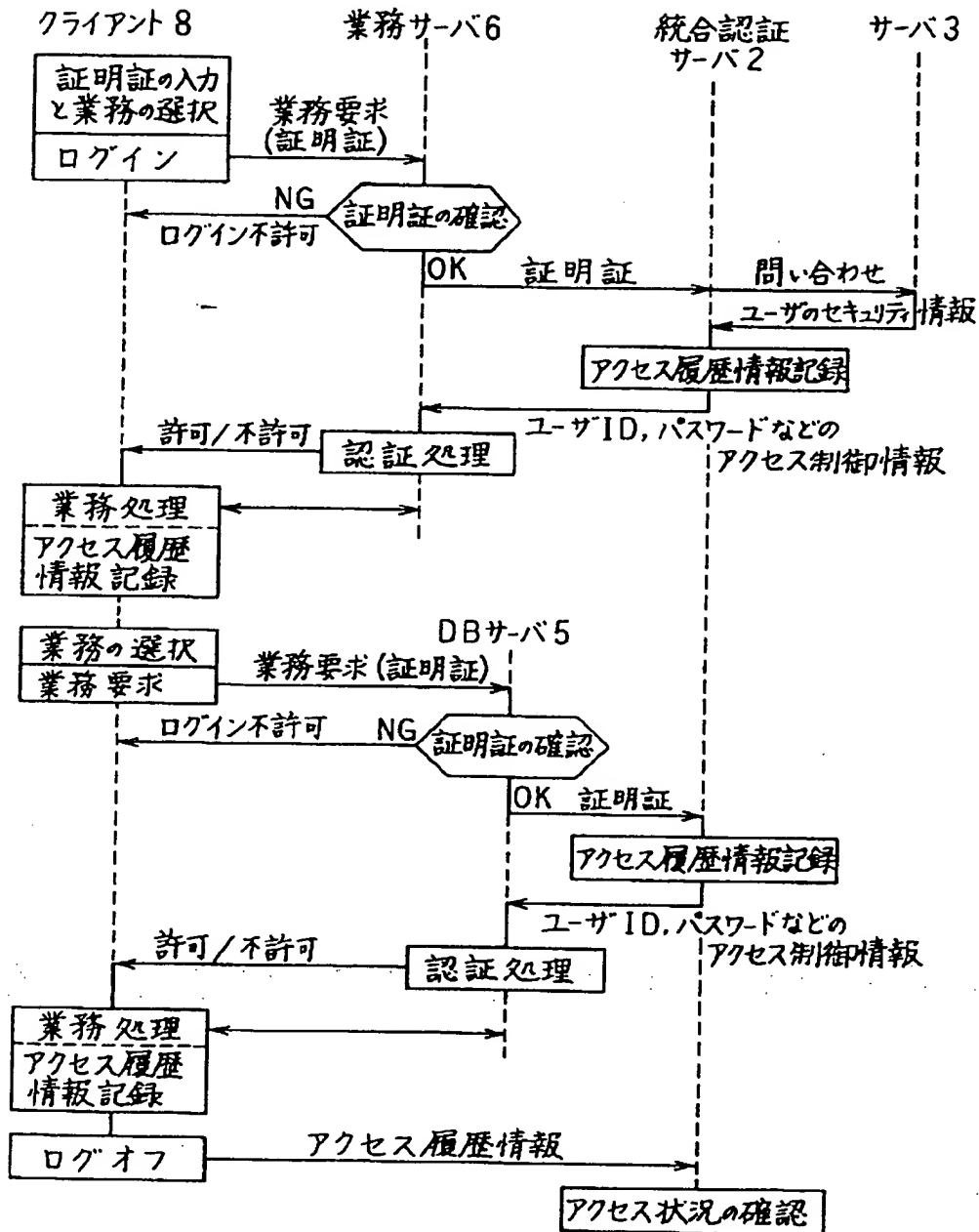
【図5】

図5



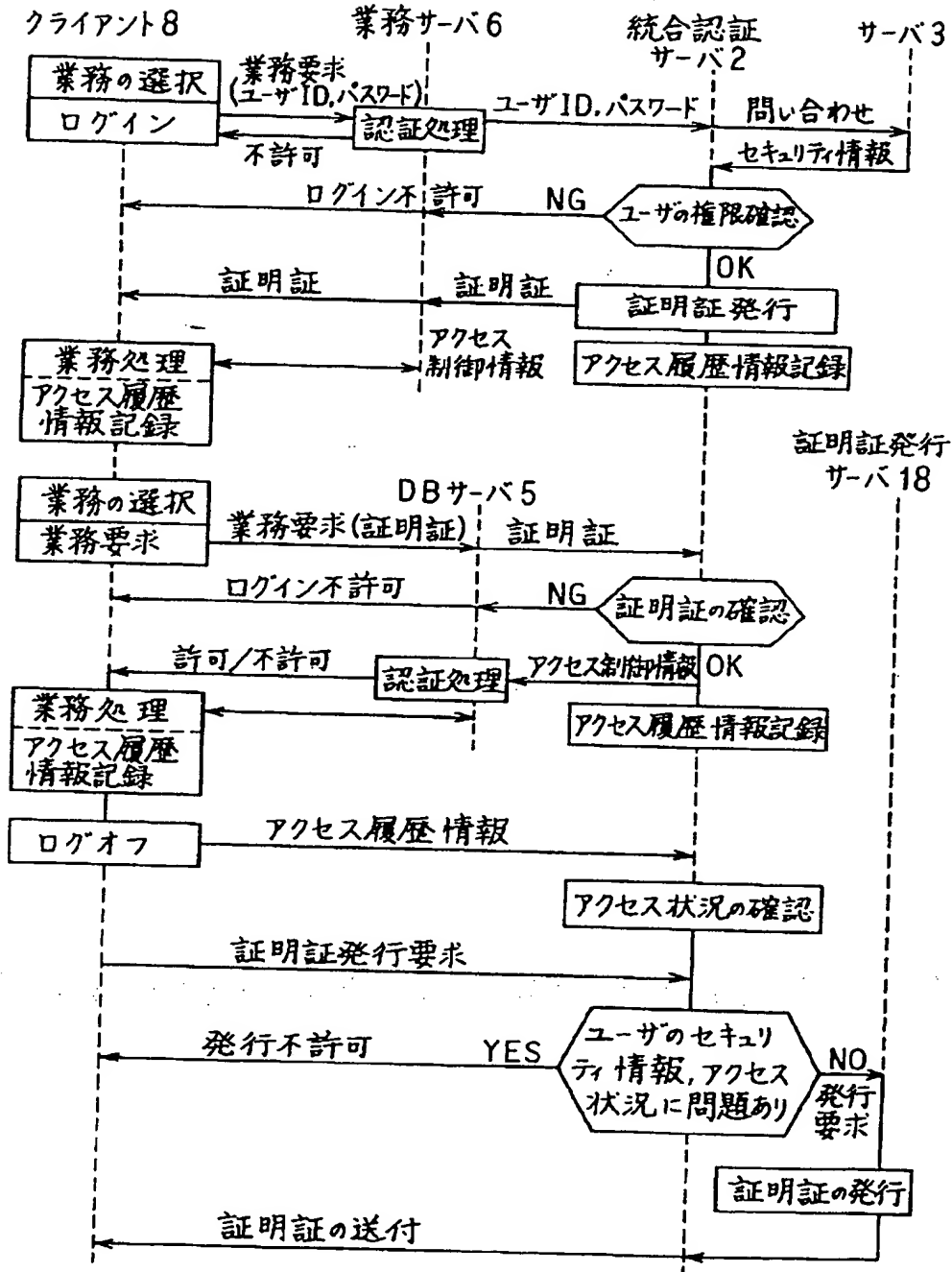
【図6】

図 6



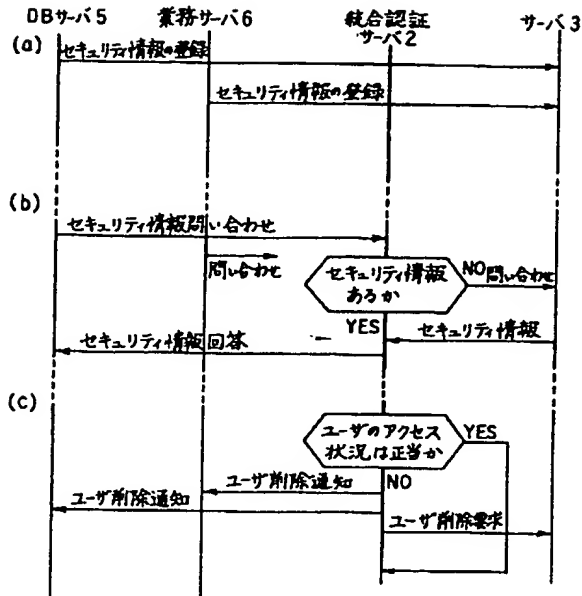
【図7】

図7



【図9】

図9



【図10】

図10

